PacNet
Number 75

Pacific Forum CSIS
Honolulu, Hawaii

Nov. 3, 2015

Critical threats to the internet by Fergus Hanson

Fergus Hanson is author of Internet Wars, the struggle for power in the 21st century and is a non-resident fellow at the Brookings Institution. You can follow him at @fergushanson.

What's the most valuable piece of global real estate? The internet is a contender. When Chinese President Xi Jinping visited the United States last month, his government's rapacious online theft of intellectual property topped the agenda. The latest Worldwide Threat Assessment, the US intelligence community's analysis of global treats, put cyber threats first, ahead of weapons of mass destruction and terrorism.

Forget the adorable cats: the internet is reshaping global power dynamics. The world's first universal network offers the promise of immense power to the countries and companies that control it, driving a contest with grave risks to the internet. Two demand urgent attention.

'The greatest transfer of wealth in history'

State-backed theft of Western intellectual property has reached such staggering proportions that dangerous escalation is all but inevitable without a new global consensus. Keith Alexander, the former head of the National Security Agency, has said that economic cyber espionage has led to "the greatest transfer of wealth in history." A private Commission on the Theft of American Intellectual Property reckoned that annual losses from cyber theft are equal to the value of all US exports to Asia – over $300 billion. The NSA identified more than 600 US private and government entities targeted by Chinese cyber attacks over the last five years.

This slow bleeding of the US economy has forced the administration's hand. In May 2014, the Justice Department issued five arrest warrants for members of the Chinese military alleged to have hacked US companies. When that signal was ignored, the US discussed economic sanctions. To forestall this, China dispatched a senior official ahead of Xi's September visit who managed to hash out a deal during last-minute talks with National Security Adviser Susan Rice and the US secretaries of state and homeland security.

During the visit, Presidents Obama and Xi announced a verbal agreement to cease conducting or knowingly supporting "cyber-enabled theft of intellectual property" as well as progress on related law enforcement. Remarkably, the *Washington Post* soon reported that "The Chinese government has quietly arrested a handful of hackers at the urging of the U.S. government … accused of carrying out state-sponsored economic espionage."

This is unlikely to be enough. For a start, there are other reasons for attacking a US company besides stealing IP. In April a new offensive tool in China's arsenal was identified, "the Great Cannon," which it used against selected pages of GitHub, a code-sharing site. This included pages that monitor Chinese online censorship, and a Chinese language version of the *New York Times*. As the Citizen Lab report that identified the weapon stated: the Cannon "manipulates the traffic of 'bystander' systems outside China, reprogramming their browsers to create a massive DDoS [distributed denial of service] attack," in effect using it to deny other users access to those webpages. Another reason could be revenge: in 2014, Iranian hackers launched a cyber attack on Las Vegas Sands casino in an apparent attempt to get back at its CEO and majority owner Sheldon Adelson for comments he'd made about Iran.

The agreement also excludes other significant perpetrators (and victims). As James Clapper stated in his report to the Senate Armed Services Committee: "several nations – including Iran and North Korea – have undertaken offensive cyber operations against private sector targets to support their economic and foreign policy objectives." He also noted "the Russian cyber threat is more severe than we had previously assessed."

Without a more comprehensive agreement, sanctions and other measures will likely remain on the table.

Waging war in peacetime

It was only mid-2009 when the secretary of defense ordered the establishment of a dedicated US Cyber Command. Now more than 100 countries have military and intelligence cyber warfare units. In the words of then-Chairman of the Joint Chiefs of Staff Martin Dempsey, cyber has become "one of the most serious threats to national security." A key problem is the absence of well-accepted norms of behavior spanning both its use in conflicts and, more worrying, a broad spectrum of peacetime scenarios.

There appears to be an emerging norm permitting cyber attacks during peacetime. In 2012, the United Kingdom's then-Minister of State for the Armed Forces Nick Harvey even made the case to the Shangri-La Dialogue that cyber attacks were "quite a civilised option."

Practice would suggest several states agree. In 2012, it was revealed the United States and likely Israel had been targeting Iran's nuclear program with cyber attacks: the first time a cyber attack had turned hot, doing physical real-world damage. In retaliation, Iran launched a major cyber attack in August 2012 on the world's largest energy company, Saudi Aramco, releasing a virus, dubbed Shamoon, which replicated itself across 30,000 Saudi Aramco computers and took almost two weeks to recover from.

North Korea has also been active. In November 2014, it struck at Sony after the company proceeded with its movie, *The Interview*, which fantasized the assassination of the North

Korean leader. The attackers used the threat of terrorism to persuade theater chains in the United States to pull out of screening the film. And in March 2015, South Korea formally accused the North of cyber attacks on its nuclear reactor operator that occurred in December 2014.

These attacks didn't lead to any deaths, but it is only a matter of time. Major attacks on critical infrastructure could easily result in many deaths, making escalation to traditional military options possible.

None of these issues are easily solved, but without action the internet will become a different beast as states are forced to take defensive measures. In a worst-case scenario that means a Balkanization of the internet into walled-off communities.

Many reflexively look to the UN. While it brings every state to the table, it excludes critical actors from voting, like internet-governing bodies and major IT companies. It is also vulnerable to efforts by some states to reduce protections for human rights and free speech.

A better option, especially for countering economic cyber espionage, would be the G-20, which brings together key states, the private sector, and civil society (through the B-20 and C-20). It operates more informally, lending itself to an area where agreed norms of behaviour are desperately needed, but formal agreement unlikely for many years.

PacNet commentaries and responses represent the views of the respective authors. Alternative viewpoints are always welcomed and encouraged.